REMARKS

The present application and its claims are directed to a mobile application security system and method. Claims 1-19 were originally filed and Claim 20 has been added so that Claims 1- 20 are presented for the Examiner's consideration.

INFORMATION DISCLOSURE STATEMENT

Applicant is submitting herewith an Information Disclosure Statement ("IDS") that Applicant requests that the Examiner consider. The IDS contains several of the same articles previously submitted, but Applicant noted that the publication date of those articles was not listed on the 1449 form and decided to re-submit these articles.

PRIOR ART REJECTIONS

In response to the Examiner's rejection of Claims 1- 19 under 35 U.S.C. 102(a) as being anticipated by Jansen et al., NIST Special Publication 800-19- Mobile Application Security (hereinafter "Jansen"), Applicant respectfully traverses the rejection. In particular, the claims are not anticipated by Jansen for the reasons set forth below and early allowance of the claims is respectfully requested.

Claim 1 and 10

Claim 1 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein the mobile application is communicated from a first host to a second host through the central computer" as set forth in the claim. To support the rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen describes a Jumping Beans system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer that enforces security as each host must performs its own security and reject a mobile agent. The Jumping Beans system as described in the Jansen article has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is

communicated from a first host to a second host through the central computer. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central computer as set forth in the claim through which a mobile application is sent as the mobile application jumps between hosts and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Claim 1 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support the rejection of this element of Claim 1. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central computer that monitors the security of the mobile application nor a central computer that detected unwanted changes as claimed.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Nothing in this section of Jansen teaches or suggests that a central computer detects unwanted changes in the code associated with the mobile application when the mobile application is jumping between hosts as set forth in the claim. Thus, Jansen does not disclose or suggest the invention recited in Claim 1. Claims 10 is allowable over Jansen for at least the same reasons as Claim 1.

Claims 2 and 11

Claim 2 is allowable for at least the same reasons as Claim 1 above. In addition, Claim 2 is not anticipated by Jansen as Jansen does not teach that a central computer stores a copy of a

mobile application and then compares it to the mobile application after execution by another host as set forth in the claim. To support the rejection, the Examiner cites to Section 3.2 of Jansen and states "1st paragraph teaches protecting against modification of code, ie. comparing the original to the one received." However, the second portion of the statement by the Examiner does not logically follow from the first part as there are many different ways to protect against code modification and the first statement does not, in any way, disclose, imply or suggest the conclusion made by the Examiner. Therefore, Section 3.2 does not support the Examiner's rejection.

Furthermore, the Examiner has relied on Section 4.2.2 of Jansen that discusses mutual itinerary recording to support his rejection. However, Section 4.2.2 describes that the itinerary of the mobile agent is recorded by another agent and used to detect malicious platform behavior. However, this section of Jansen does not describe that the copy of the mobile agent (which is different from the itinerary) is made at the central computer and then the central computer uses the stored copy to compare to the mobile application after it has been executed by another host. Jansen's system attempts to catch inconsistencies in the itineraries of the mobile agents, but would not detect other code modifications of the mobile agent. In addition, the system in Jansen does not describe that the elements set forth in this claim are at the central computer as claimed.

Finally, the Examiner cites to the lists/tables at the bottom of page 14 and at the top of page 19 in Jansen to support the rejection of this claim. However, none of the items listed on page 14 or page 19 disclose (or even suggest) that a central computer stores a copy of a mobile application and then compares it to the mobile application after execution by another host as set forth in the claim. It is thus hard to imagine how one of ordinary skill in the art, based on the disclosure in Jansen, would implement the claimed mobile application comparison element when it is not even suggested in the Jansen article. Thus, the lists do not support the Examiner's rejection of this claim and Claim 2 is allowable over Jansen.

Similarly, Claim 11 is allowable over Jansen for at least the same reasons as Claim 1 and is further allowable over Jansen for at least the same reasons as Claim 2 above.

Claims 3 and 12

Claim 3 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile

application as it jumps between the host computers wherein the mobile application is communicated from a first host to a second host through the central computer" as set forth in the claim. To support the rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen describes a Jumping Beans system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer that enforces security as each host must performs its own security and reject a mobile agent. The Jumping Beans system as described in the Jansen article has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host through the central computer. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central computer as set forth in the claim through which a mobile application is sent as the mobile application jumps between hosts and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Jansen does not teach "wherein the security monitoring means further comprises means for preventing a host from transmitting hostile code in a mobile application to another host." The Examiner has cited to the IBM Aglets discussion on page 19 of Jansen to support his rejection of this element of the claim. However, it is clear from the description that the Aglets system does not have a central computer and that the Aglets system does not have a central computer that prevents a host from transmitting hostile code in a mobile application to another host. In the Aglets system, each host has its own security system (not a central computer with a security monitor) and each host must block the mobile application which is different from a central computer preventing a host for transmitting hostile code in a mobile application. In addition, the Aglets system does not prevent a host from transmitting the hostile code as claimed, but only blocks the mobile application being accepted at a particular host. So, the Aglets system permits the mobile application with hostile code to be transmitted to a host and expects the host to block the mobile application while the invention prevents the transmission of the mobile

application and does not require that each host has a security module. For the Jumping Beans system mentioned in Jansen, it does not prevent a host from transmitting hostile code in a mobile application to another host. Therefore, Claim 3 is allowable over Jansen. Claim 12 is allowable over Jansen for at least the same reasons as Claim 3.

Claims 4 and 13

Claim 4 is allowable over Jansen for at least the same reasons as Claim 3. In addition, Jansen does not disclose "means for stripping the code from an initially received mobile application if the host is not trusted, means for saving the code of the mobile application, and means, when requested by another host, for providing the code for the mobile application to the requesting host" as set forth in the claim. When faced with supporting a rejection of the "means for stripping code" element, the Examiner states that "many options exist as to how to stay safe from said machine [the untrusted host]..." and explains why stripping code is a harsh remedy and should be left to a system administrator on page 4 of the Office action. However, the Examiner never cites to a portion of Jansen that specifically discloses the "means for stripping" element set forth in Claim 4 nor that the element resides on a central computer. In fact, Jansen does not disclose the elements recited in Claim 4 and therefore Claim 4 is allowable over Jansen. Claim 13 is allowable over Jansen for at least the same reasons.

Claims 5 and 14

Claim 5 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein the mobile application is communicated from a first host to a second host through the central computer" as set forth in the claim. To support the rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen describes a Jumping Beans system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer that enforces security as each host must performs its own security and reject a mobile agent. The Jumping Beans system as described in the Jansen article has a secure central host, but Jansen does not describe that the

Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host through the central computer. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central computer as set forth in the claim through which a mobile application is sent as the mobile application jumps between hosts and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Claim 5 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the state of the mobile application." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support the rejection of this element of Claim 5. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central computer that monitors the security of the mobile application nor a central computer that detects unwanted changes in the state of the mobile application.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Nothing in this section of Jansen teaches or suggests that a central computer detects unwanted changes in the state of the mobile application when the mobile application is jumping between hosts as set forth in the claim. Thus, Jansen does not disclose or suggest the invention recited in Claim 5. Claims 14 is allowable over Jansen for at least the same reasons as Claim 5.

Claims 6 and 15

Claim 6 is allowable for at least the same reasons as Claim 5 above. In addition, Claim 6 is not anticipated by Jansen as Jansen does not teach that a central computer stores a copy of the state of a mobile application and then compares it to the state of a mobile application from another host as set forth in the claim. To support the rejection, the Examiner cites to Section 3.2 of Jansen and states "1st paragraph teaches protecting against modification of code, ie. comparing the original to the one received." However, the second portion of the statement by the Examiner does not logically follow from the first part as there are many different ways to protect against code modification and the first statement does not, in any way, disclose, imply or suggest the conclusion made by the Examiner. Therefore, Section 3.2 does not support the Examiner's rejection.

Furthermore, the Examiner has relied on Section 4.2.2 of Jansen that discusses mutual itinerary recording to support his rejection. However, Section 4.2.2 describes that the itinerary of the mobile agent is recorded by another agent and used to detect malicious platform behavior. However, this section of Jansen does not describe that the copy of the state of the mobile agent (which is different from the itinerary) is made at the central computer and then the central computer uses the stored copy of the state to compare to the state of a mobile application after execution by another host. Jansen's system attempts to catch inconsistencies in the itineraries of the mobile agents, but would not detect other code modifications of the mobile agent. In addition, the system in Jansen does not describe that the elements set forth in this claim are at the central computer as claimed.

Finally, the Examiner cites to the lists/tables at the bottom of page 14 and at the top of page 19 in Jansen to support the rejection of this claim. However, none of the items listed on page 14 or page 19 disclose (or even suggest) that a central computer stores a copy of the state of a mobile application and then compares the state to the state of the mobile application after execution by another host as set forth in the claim. It is thus hard to imagine how one of ordinary skill in the art would use the claimed mobile application comparison element when it is not even suggested in the Jansen article. Thus, the lists do not support the Examiner's rejection of this claim and Claim 6 is allowable over Jansen.

Similarly, Claim 15 is allowable over Jansen for at least the same reasons as Claim 5 and is further allowable over Jansen for at least the same reasons as Claim 6 above.

Claims 7- 9 and 16-18

Claim 7 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein the mobile application is communicated from a first host to a second host through the central computer" as set forth in the claim. To support the rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen describes a Jumping Beans system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer that enforces security as each host must performs its own security and reject a mobile agent. The Jumping Beans system as described in the Jansen article has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host through the central computer. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central computer as set forth in the claim through which a mobile application is sent as the mobile application jumps between hosts and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

In addition, Claim 7 is not anticipated by Jansen for the reason that Jansen does not disclose "the security monitoring means further comprises means for detecting unwanted changes in the itinerary of the mobile application when the mobile application is jumping between hosts." The Examiner has cited Sections 2.2.4 and 2.3.4 of Jansen to support his rejection of this element of Claim 7. Section 2.2.4 teaches that the modification of an agent's code is a particularly insidious form of attack. Jansen also describes using signed code to solve this problem. However, the signed code described in Jansen does not permit a trusted host to modify the code of a mobile application (as it might do), requires each host to maintain a list of

the trusted hosts and requires the secure distribution of the public keys. This signed code is not a central computer that monitors the security of the mobile application nor a central computer that detects unwanted changes in the itinerary of the mobile application.

Section 2.3.4 of Jansen teaches that a platform must be prevented from modifying an agent's code, state or data without being detected and describes some examples of this problem. Jansen also describes that an original author can sign the agent's code to prevent changes in the code. Jansen then describes that a multi-hop scenario is more risky than a single hop problem. Thus, in Section 2.3.4, Jansen teaches 1) that code modification is bad; 2) that a digital signature may prevent some code modification; and 3) that multi-hop risks are higher since the mobile application is farther away from its home platform. Although Jansen does discuss that the itinerary of a mobile agent may be stored, Jansen does not disclose that the itinerary of the mobile agent is stored at a central computer or that the central computer detected unwanted changes in the itinerary of the mobile application. Thus, Jansen does not disclose or suggest the invention recited in Claim 7. Claims 8 and 9 are allowable over Jansen for at least the same reasons as Claim 7.

Claim 16 is allowable for at least the same reasons as Claim 7 above and Claims 17-18 are allowable for at least the same reasons as Claims 8-9 above.

Claims 19 - 20

Claim 19 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein the mobile application is communicated from a first host to a second host through the central computer" as set forth in the claim. To support the rejection, the Examiner cites to pages 13-14 and 18-19. At pages 13-14, Jansen teaches a "reference monitor" that establishes separate isolated domains for each agent and the platform and controls all inter-domain access. At pages 18-19, Jansen describes a Jumping Beans system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central computer that enforces security as each host must performs its own security and reject a mobile agent. The Jumping Beans system as described in the Jansen article has a secure central host, but Jansen does not describe that the

Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central computer when the mobile application is communicated from a first host to a second host through the central computer. Furthermore, the description of the reference monitor does not describe that the reference monitor is a central computer as set forth in the claim through which a mobile application is sent as the mobile application jumps between hosts and does not teach the elements set forth in the claim. Thus, Jansen does not teach this element.

Furthermore, Jansen does not disclose "wherein the security monitoring further comprises preventing untrusted hosts from initially launching mobile applications" as set forth in the claim. The Examiner points out that "a non-trusting host launching a mobile application reads on hostile code" in the rejection. Even assuming that the above statement is correct (which it is not), it is unclear how Jansen therefore discloses that the central computer prevents untrusted hosts from initially launching mobile applications as claimed. At most, Jansen describes the Aglet system that blocks an incoming mobile application which is very different from a central computer that prevents untrusted hosts from initially launching mobile applications as set forth above. Thus, Jansen does not disclose this feature and therefore Claim 19 is allowable over Jansen.

Claim 20 is allowable over Jansen for at least the same reasons as Claim 19.

CONCLUSION

In view of the above, it is respectfully submitted that Claims 1-20 are allowable over the prior art cited by the Examiner and early allowance of these claims and the application is respectfully requested.

The Examiner is invited to call Applicant's attorney at the number below in order to speed the prosecution of this application.

The Commissioner is authorized to charge any deficiencies in fees and credit any overpayment of fees to Deposit Account No. 07-1896.

Respectfully submitted,

GRAY CARY WARE & FREIDENRICH LLP

Dated: March 19, 2004 By _____

Timothy W. Lohse
Reg. No. 35,255
Attorney for Applicant

GRAY CARY WARE & FREIDENRICH
2000 University Avenue
East Palo Alto, CA 94303
Telephone: (650) 833-2055

Gray Cary\EM\7161960.1
1010722-991100

Gray Cary\EM\7161960.1
1010722-991100